UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/873,339	06/05/2001	Timothy P. Barber	01,204	4133

7590 06/15/2005	EXAMINER
SHUGHART THOMSON & KILROY, P.C.	SHINGLES, KRISTIE D

SHUGHART THOMSON & KILROY, P.C.
Twelve Wyandotte Plaza
120 West 12th Street
Kansas City, MI 64105

ART UNIT	PAPER NUMBER
2141	

DATE MAILED: 06/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/873,339	BARBER, TIMOTHY P.
	Examiner	Art Unit	
	Kristie D. Shingles	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Response to Amendment

Applicant has amended claims 1-26 therefore claims 1-26 are now pending.

Response to Arguments

1.   Applicant's arguments with respect to claims 1-26 have been considered but are moot in

view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

3.   Claims 1-26 rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent

6,535,916 to Nguyen in view of Cooper et al (US 5,563,946).

Regarding claim 1, Nguyen teaches a process for collecting machine identifying

information associated with a digital online access device used for substantially anonymously

accessing a host computer system over a digital network said host computer system generating

an interaction record of an access therewith by said access device, and said process comprising:

(a) capturing a machine fingerprint that identifies said access device accessing said host

computer system; (b) generating a unique interaction identification string upon said access

device accessing said host computer system (column 5, lines 18-27 and 32-37); (c) associating

said interaction identification string with said machine fingerprint; and (d) associating said

interaction identification string with said interaction record generated upon said access device

accessing said host computer system (column 5, line 65-column 6, line 4 and column 6, lines 8-

12).

Nguyen does not teach wherein said machine fingerprint comprises a hashed attribute

string that is a concatenation of attributes associated with said access device. Cooper et al.

teaches wherein said machine fingerprint comprises a hashed attribute string that is a

concatenation of attributes associated with said access device (column 7, lines 55-63, column 15,

lines 30-34, column 23, lines 37-47, column 26, lines 54-58). Therefore it would have been

obvious to one of ordinary skill in the art at the time the invention was made to further modify

the online machine data collection process of Nguyen by wherein said machine fingerprint

comprises a hashed attribute string that is a concatenation of attributes associated with said

access device because this assist in combating against fraud by accurately identifying the

computer through which customers make transactions and associating said identity with

suspicious transactions (pg.2 lines 8-10 of Applicant Admitted Prior Art).

Regarding claim 7, Nguyen teaches a process for identifying a customer computer

involved in an online transaction between a customer using a customer browser operating on said

customer computer and a merchant operating a merchant web site, said method comprising the

steps of: (a) capturing a machine fingerprint of a customer computer upon said customer

computer accessing said merchant web site; (b) generating a transaction identification string and

associating said string with said machine fingerprint (column 5, lines 18-27 and 32-37); (c)

storing said machine fingerprint and said string in a machine data archive; (d) upon said

customer completing a transaction through said merchant web site, storing said transaction

identification string with a transaction record formed during said transaction to thereby associate

said parameter with said transaction record through said transaction identification string (column

5, line 65-column 6, line 4 and column 6, lines 8-12 and 16-23).

Nguyen does not teach wherein said machine fingerprint comprises a hashed attribute

string that is a concatenation of attributes associated with said access device. Cooper et al.

teaches wherein said machine fingerprint comprises a hashed attribute string that is a

concatenation of attributes associated with said access device (column 7, lines 55-63, column 15,

lines 30-34, column 23, lines 37-47, column 26, lines 54-58). Therefore it would have been

obvious to one of ordinary skill in the art at the time the invention was made to further modify

the online machine data collection process of Nguyen by wherein said machine fingerprint

comprises a hashed attribute string that is a concatenation of attributes associated with said

access device because this assist in combating against fraud by accurately identifying the

computer through which customers make transactions and associating said identity with

suspicious transactions (pg.2 lines 8-10 of Applicant Admitted Prior Art).

Regarding claim 16, Nguyen teaches a process for identifying a customer computer

involved in an online transaction through a merchant web site between a customer using a

customer browser operating on said customer computer and a merchant who operates said web

site, said method comprising the steps of: (a) coding a script request within a transaction form of

said merchant web site; (b) processing said script request by said customer browser upon

accessing said merchant web site to thereby communicate to an archiver web site of a machine

data archiving service an electronic request for a machine data collection script; (c) said archiver

web site returning said script to said customer browser along with a unique transaction

identification string (column 5, lines 32-37); (d) said customer browser processing said script to

thereby cause said script to query said customer computer for a machine fingerprint of said

customer computer; (e) said script causing said customer browser to communicate said machine

fingerprint and said transaction identification string to said archiver web site; (f) said archiver

web site storing said machine fingerprint and said transaction identification string in a machine

data profile (column 6, lines 16-22); (g) said script causing said customer browser to write said

transaction identification string into said transaction form (column 6, lines 8-12); and (h) upon

said customer adding customer identification information to said transaction form and

electronically submitting said transaction form to said merchant web site to thereby comprise a

transaction record, said transaction identification string associating said transaction record with

said machine data profile (column 5, lines 20-27 and column 5, line 65-column 6, line 4).

Nguyen does not teach wherein said machine fingerprint comprises a hashed attribute

string that is a concatenation of attributes associated with said access device. Cooper et al.

teaches wherein said machine fingerprint comprises a hashed attribute string associated with one

or more attributes of said customer computer (column 7, lines 55-63, column 15, lines 30-34,

column 23, lines 37-47, column 26, lines 54-58). Therefore it would have been obvious to one of

ordinary skill in the art at the time the invention was made to further modify the online machine

data collection process of Nguyen by wherein said machine fingerprint comprises a hashed

attribute string that is a concatenation of attributes associated with said access device because

this assist in combating against fraud by accurately identifying the computer through which

customers make transactions and associating said identity with suspicious transactions (pg.2 lines

8-10 of Applicant Admitted Prior Art).

Regarding claim 24, Nguyen teaches a process for identifying a customer computer

involved in an online transaction through a merchant web site between a customer using a

customer browser operating on said customer computer and a merchant who operates said web

site, said method comprising the steps of (a) coding a script request within a transaction form of

said merchant web site (column 6,lines 8-12); (b) processing said script request by said customer

browser upon accessing said merchant web site to thereby communicate to an archiver web site

of a machine data archiving service an electronic request for a machine data collection script; (c)

said archiver web site returning said script to said customer browser along with a unique

transaction identification string (column 5, line 65-column 6, line 4); (e) said script causing said

customer browser to communicate said machine fingerprint, said time value, and said transaction

identification string to said archiver web site along with a conventional HTTP header (column 5,

lines 33-37 and 45-47); (f) said archiver web site storing said machine fingerprint, said time

value, and said transaction identification string in a machine data profile (column 6, lines 16-22);

(g) said script causing said customer browser to write said transaction identification string into

said transaction form; and (h) upon said customer adding customer identification information to

said transaction form and electronically submitting said transaction form to said merchant web

site to thereby comprise a transaction record, said transaction identification string associating

said transaction record with said machine data profile (column 5, lines 19-27).

Nguyen does not teach configuration settings. Cooper et al. teaches (d) said customer

browser processing said script to thereby cause said script to: (1) query said customer browser

for a plurality of configuration settings; (2) form an attribute string from said plurality of

configuration settings; (3) perform a hashing function on said attribute string to form a machine

fingerprint of said customer computer; and (4) query an internal digital clock of said customer

computer for a current time value; (column 7, lines 55-63, column 15, lines 30-34, column 23,

lines 37-47, column 26, lines 54-58). Therefore it would have been obvious to one of ordinary

skill in the art at the time the invention was made to further modify the online machine data

collection process of Nguyen by (d) said customer browser processing said script to thereby

cause said script to: (1) query said customer browser for a plurality of configuration settings; (2)

form an attribute string from said plurality of configuration settings; (3) perform a hashing

function on said attribute string to form said machine fingerprint; and (4) query an internal

digital clock of said customer computer for a current time value because this assist in combating

against fraud by accurately identifying the computer through which customers make transactions

and associating said identity with suspicious transactions (pg.2 lines 8-10 of Applicant Admitted

Prior Art).

Regarding claim 3 and 18, Nguyen teaches a process as set forth in Claim 1 and 16

(column 5, lines 19-27).

Nguyen does not teach configuration settings. Cooper et al. teaches wherein said hashed

attribute string comprises: (a) a configuration setting of said access device (column 7, lines 55-

63, column 15, lines 30-34, column 23, lines 37-47, column 26, lines 54-58). Therefore it would

have been obvious to one of ordinary skill in the art at the time the invention was made to further

modify the online machine data collection process of Nguyen by wherein said capturing step

includes the step of: (a) capturing a configuration setting of said access device because the

configuration settings of a computer system are another form of uniquely identifying that system.

Regarding claim 4 and 12, Nguyen teaches a process as set forth in Claim 1 and 7 further

comprising: (a) communicating a self-identification routine to said access device upon said

access device accessing said host computer system; (b) said access device executing said self-

identification routine; and (d) said self-identification routine communicating said machine

fingerprint to a remote location for association with said interaction identification string (column

5, lines 19-27).

Nguyen does not teach configuration settings. Cooper et al. teaches (c) said self-

identification routine querying a configuration setting of said access device to derive said

machine fingerprint (column 7, lines 55-63, column 15, lines 30-34, column 23, lines 37-47,

column 26, lines 54-58). Therefore it would have been obvious to one of ordinary skill in the art

at the time the invention was made to further modify the online machine data collection process

of Nguyen by(c) said self-identification routine querying a configuration setting of said access

device to derive said machine fingerprint because the configuration settings of a computer

system are another form of uniquely identifying that system.

Regarding claim 9, Nguyen teaches a process as set forth in Claim 7 (column 5, lines 19-

27).

Nguyen does not teach configuration settings. Cooper et al. teaches wherein said machine

fingerprint comprises: a configuration setting of said customer computer (column 7, lines 55-63,

column 15, lines 30-34, column 23, lines 37-47, column 26, lines 54-58). Therefore it would

have been obvious to one of ordinary skill in the art at the time the invention was made to further

modify the online machine data collection process of Nguyen by wherein said capturing step

includes the step of: (a) capturing a configuration setting of said customer computer because the

configuration settings of a computer system are another form of uniquely identifying that system.

Regarding claim 14 and 19, Nguyen teaches a process as set forth in Claim 12 and 16

(column 5, lines 19-27).

Nguyen does not teach configuration settings. Cooper et al. teaches wherein said

querying step further comprises: (a) querying said customer browser for a plurality of

configuration settings: (b) forming an attribute string from said plurality of configuration

settings; and (c) hashing said attribute string to form said machine fingerprint of said customer

computer (column 7, lines 55-63, column 15, lines 30-34, column 23, lines 37-47, column 26,

lines 54-58). Therefore it would have been obvious to one of ordinary skill in the art at the time

the invention was made to further modify the online machine data collection process of Nguyen

by wherein said querying step includes the steps of: (a) querying said customer browser for a

plurality of configuration settings: (b) forming an attribute string from said plurality of

configuration settings; and (c) hashing said attribute string to form said machine fingerprint of

said customer computer because the configuration settings of a computer system are another

form of uniquely identifying that system.

Regarding claim 2, Nguyen teaches a process as set forth in Claim 1 further comprising:

(a) capturing a digital address of said access device on said digital network (column 5, lines 19-

27 and 32-37).

Regarding claim 5, Nguyen teaches a process as set forth in Claim 1 further comprising:

(a) said host system operating a host web site including an interaction page generated by

interaction page code processed by said access device upon accessing said host web site; and (b)

coding, within said interaction page code, a self-identification routine which causes said access

device to communicate said machine fingerprint when said access device processes said

interaction page code (column 5, lines 19-27 and 32-37 and 44-47).

Regarding claim 6, Nguyen teaches a process as set forth in Claim 3 further comprising:

(a) coding said self-identification routine in such a manner that said machine fingerprint and said

interaction identification string are communicated to a third party web site at which said machine

fingerprint and said interaction identification string are stored (column 5, lines 19-27 and column

6, lines 16-22).

Regarding claim 8, Nguyen teaches a process as set forth in Claim 7 further comprising:

(a) capturing an IP address of said customer computer (column 5, lines 19-27 and 32-37).

Regarding claim 10, 11 and 13, Nguyen teaches a process as set forth in Claim 7 and 12

comprising: (a) coding said self-identification routine in such a manner that said machine

fingerprint and said interaction identification string are communicated to a third party web site at

which said machine fingerprint and said interaction identification string are stored (column 5,

lines 19-27 and column 6, lines 16-22).

Regarding claim 15, Nguyen teaches a process as set forth in Claim 12 wherein said

customer computer potentially accesses said merchant web site by way of a proxy, and said

communicating step further comprises: (a) communicating said machine fingerprint and said

transaction identification string to said remote web site using a protocol which bypasses said

proxy (column 5, lines 19-27 and column 6, lines 16-22).

Regarding claim 17, Nguyen teaches a process as set forth in Claim 16 further comprising: (a) said script causing said computer browser to communicate said machine fingerprint and said transaction identification string along with a conventional hypertext transfer protocol (HTTP) header; and (b) said archiver service additionally storing said HTTP header in association with said machine data profile (column 5, lines 19-27 and 45-47).

Regarding claim 20, Nguyen teaches a process as set forth in Claim 19 further comprising: (a) said script performing a hashing function on said attribute string to form said machine fingerprint (column 5, lines 19-27).

Regarding claim 21, Nguyen teaches a process as set forth in Claim 16 wherein said customer computer potentially accesses said merchant web site by way of a proxy, said process further comprising: (a) communicating said machine fingerprint and said transaction identification string to said remote web site using a protocol which bypasses said proxy (column 5, lines 19-27 and column 6, lines 16-22).

Regarding claim 22, Nguyen teaches a process as set forth in Claim 16 further comprising: (a) said script communicating said machine fingerprint to said archiver service web site using a protocol other than HTTP (column 5, lines 19-27 and 45-47).

Regarding claim 23, Nguyen teaches a process as set forth in Claim 16 wherein said customer computer comprises a digital clock, and further comprising: (a) said script causing said customer browser to query said clock for a time value; and (b) said script causing said customer browser to send said time value to said archiver service web site along with said machine fingerprint (column 5, lines 33-38).

Regarding claim 25, Nguyen teaches a process as set forth in Claim 24 wherein said

customer computer potentially accesses said merchant web site by way of a proxy, said process

further comprising: (a) said script querying said customer computer for a second machine

fingerprint; and (b) said script communicating said second machine fingerprint and said

transaction identification string to said archiver service web site using a protocol which bypasses

said proxy (column 5, lines 19-27 and 44-46 and column 6, lines 16-22).

Regarding claim 26, Nguyen teaches a process as set forth in Claim 25 further

comprising: (a) said script communicating said machine fingerprint to said archiver service web ·

site using a protocol other than HTTP (column 5, lines 19-27 and 45-47).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The following patents are cited to further show the state of the art with respect to online machine

data collection in general: Rieth et al. and Jovanovich et al.

1.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristie D. Shingles whose telephone number is 571-272-3888. The examiner can normally be reached on Monday-Friday 9:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on 571-272-3880. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KDS

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER